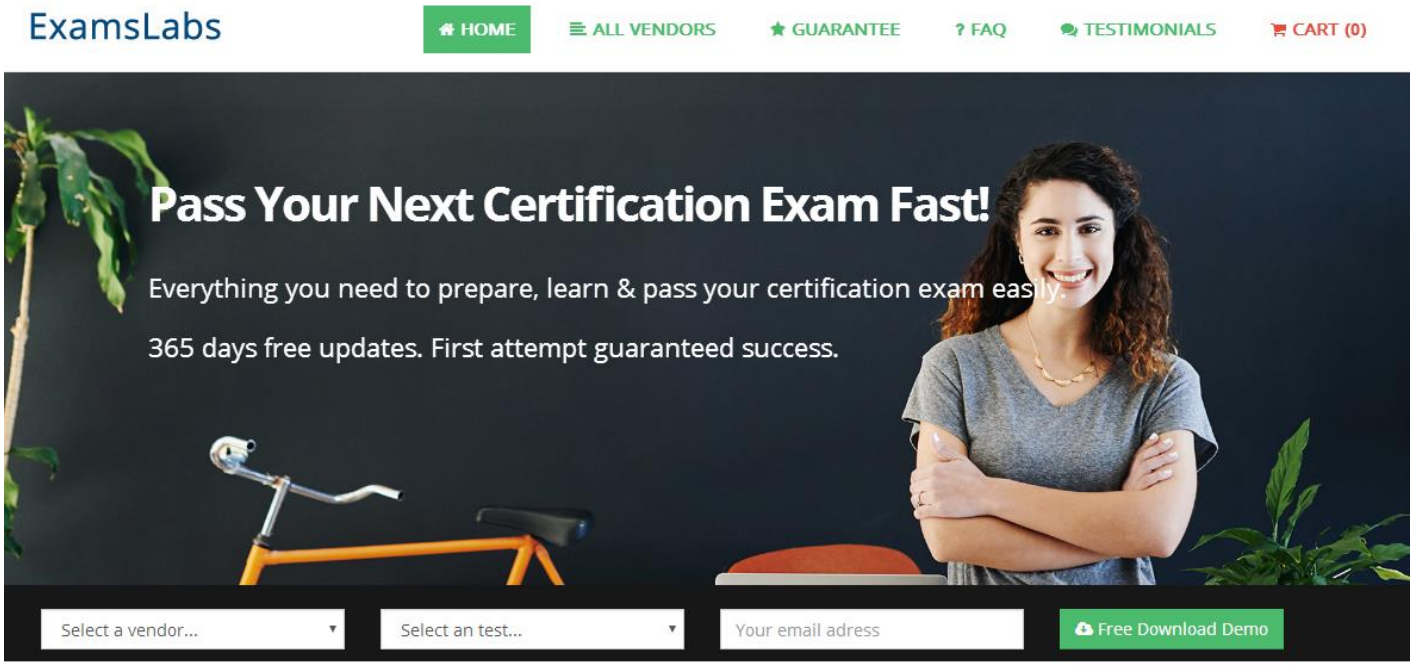
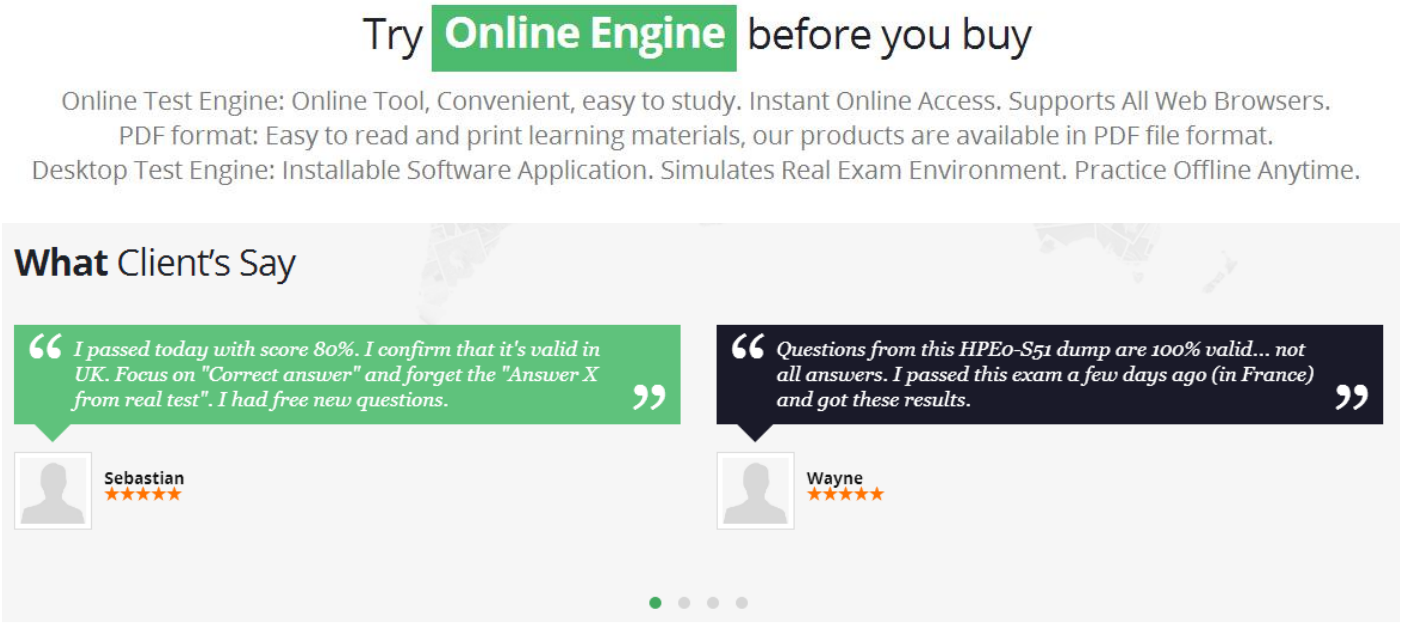
ExamsLabs





http://www.examslabs.com/

Latest Study Materials, Valid Dumps - ExamsLabs

Exam : **SCS-C01-JPN**

Title : AWS Certified Security - Specialty (SCS-C01日本語版)

Vendor : Amazon

Version : DEMO

QUESTION NO: 1
ある企業は、AWS Organizations を使用して複数の AW
アカウントを管理しています。同社は大量の機密データを処理しています。同社は、マイクロサービスに対してサーバーレス アプローチを使用しています。同社はすべてのデータを Amazon S3 または Amazon DynamoDB に保存しています。同社は、AWS
ラムダ関数、または AWS Fargate 上の Amazon Elastic Kubernetes Service (Amazon EKS) でホストしているコンテナベースのサービスを使用して、データを読み取ります。
この会社は、保管中のすべてのデータを暗号化し、最小権限のデータ
アクセス制御を適用するソリューションを実装する必要があります。会社は、AWS Key Management Service (AWS KMS) の顧客管理キーを作成します。
これらの要件を満たすために、会社は次に何をすべきでしょうか?
A. Amazon S3 および DynamoDB に対してのみ kms:Decrypt アクションを許可するキー ポリシーを作成します。キーで暗号化されていない S3 バケットと DynamoDB
テーブルの作成を拒否する SCP を作成します。
B. キーの kms:Decrypt アクションを拒否する 1AM
ポリシーを作成します。スケジュールに従って実行される Lambda
関数を作成して、ポリシーを新しいロールにアタッチします。キーで暗号化されていないリソースのアラートを送信する AWS Config ルールを作成します。
C. Amazon S3、DynamoDB、Lambda、および Amazon EKS に対してのみ kms:Decrypt アクションを許可するキー ポリシーを作成します。キーで暗号化されていない S3
バケットと DynamoDB テーブルの作成を拒否する SCP を作成します。
D. Amazon S3、DynamoDB、Lambda、および Amazon EKS に対してのみ kms:Decrypt アクションを許可するキー
ポリシーを作成します。キーで暗号化されていないリソースのアラートを送信する AWS Config ルールを作成します。
Answer: B

QUESTION NO: 2
ある企業が Amazon S3
でデータレイクを構築しています。データは、機密情報を含む何百万もの小さなファイルで構成されています。セキュリティ
チームには、アーキテクチャに関する次の要件があります。
* データは転送中に暗号化する必要があります。
* データは保存時に暗号化する必要があります。
*
バケットは非公開にする必要がありますが、バケットが誤って公開された場合、データは機密のままにする必要があります。
要件を満たすステップの組み合わせはどれですか? (3 つ選択してください。)
A. S3 バケットで Amazon S3 が管理する暗号化キー (SSE-S3)
を使用したサーバー側の暗号化を使用して、AES-256 暗号化を有効にします。
B. S3 バケットで IAM KMS マネージド キー (SSE-KMS)
を使用したサーバー側の暗号化でデフォルトの暗号化を有効にします。
C. PutObject リクエストに IAMiSecureTcanspoct
が含まれていない場合、拒否を含むバケット ポリシーを追加します。

D. ws: Sourcelpto を使用してバケット
ポリシーを追加し、企業イントラネットからのアップロードとダウンロードのみを許可します。
E. PutObject リクエストに s3:x-amz-sairv9r-side-enctyption: "IAM: kms"
が含まれていない場合、拒否を含むバケット ポリシーを追加します。
F. Amazon Macie がデータ レイクの S3
バケットへの変更を監視して対応できるようにします。
Answer: B,D,F

QUESTION NO: 3
企業のアプリケーション チームは、IAM で MySQL
データベースをホストする必要があります。同社のセキュリティ ポリシーによれば、IAM に保存されるすべてのデータは保存時に暗号化される必要があります。さらに、すべての暗号マテリアルは FIPS 140-2 レベル 3 検証に準拠している必要があります。
アプリケーション
チームは、企業のセキュリティ要件を満たし、運用オーバーヘッドを最小限に抑えるソリューションを必要としています。
これらの要件を満たすソリューションはどれですか?
A. Amazon RDS でデータベースをホストします。暗号化には Amazon Elastic Block Store (Amazon EBS) を使用します。キー管理には、IAM CloudHSM によってサポートされる IAM Key Management Service (IAM KMS) カスタム キー ストアを使用します。
B. Amazon RDS でデータベースをホストします。暗号化には Amazon Elastic Block Store (Amazon EBS) を使用します。キー管理には、IAM Key Management Service (IAM KMS) で IAM 管理の CMK を使用します。
D. Amazon EC2 インスタンスでデータベースをホストします。暗号化には Amazon Elastic Block Store (Amazon EBS) を使用します。キー管理には、IAM Key Management Service (IAM KMS) で顧客管理の CMK を使用します。
E. Amazon EC2
インスタンスでデータベースをホストします。暗号化とキー管理には透過的データ暗号化 (TDE) を使用します。
Answer: B

QUESTION NO: 4
セキュリティエンジニアは、Amazon S3 バケットポリシーを作成して、User=1、User2 という名前の IAM
ユーザーアカウントに最小権限の読み取りアクセスを付与する必要があります。とユーザー 3。これらの IAM ユーザー アカウントは、AuthorizedPeople IAM
グループのメンバーです。セキュリティ エンジニアは、次の S3 バケット
ポリシーの草案を作成します。

```
{
    "Version": "2012-10-17",
    "Id": "AuthorizedPeoplePolicy",
    "Statement": [
        {
            "Sid": "Actions-Authorized-People",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::authorized-people-bucket/*"
        }
    ]
}
```

セキュリティ エンジニアが S3 バケットにポリシーを追加しようとすると、次のエラーメッセージが表示されます:「必須フィールド プリンシパルがありません。」セキュリティエンジニアは、ポリシーに Principal 要素を追加しています。この追加では、User1のみに読み取りアクセスを提供する必要があります。ユーザー2とユーザー3。これらの要件を満たすソリューションはどれですか?

A.

```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:user/User1",
        "arn:aws:iam::1234567890:user/User2",
        "arn:aws:iam::1234567890:user/User3"
    ]
}
```

B.

```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:root"
    ]
}
```

C.

```
"Principal": {
    "AWS": [
        "*"
    ]
}
```

D.

```
"Principal": {
    "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"
}
```

Answer: A

QUESTION NO: 5
IAM Key Management Service (IAM KMS) のキー ポリシーをレビューしていたセキュリティ エンジニアが、会社の IAM アカウントの各キー
ポリシーでこのステートメントを見つけました。

```
{
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",
      "Resource": "*"
}
```

声明は何を許可していますか？
A. すべての IAM アカウントのすべてのプリンシパルがキーを使用します。
B. アカウント 111122223333 の root ユーザーのみがキーを使用します。
C. アカウント 111122223333 のすべてのプリンシパルがキーを使用しますが、Amazon S3 でのみ使用します。
D. アカウント 111122223333
のプリンシパルのみが、このキーを使用するためにこのキーへのアクセスを許可する IAM ポリシーが適用されています。
Answer: D

QUESTION NO: 6
Web
アプリケーションを使用すると、ユーザーはログインしてメンバーシップの有効性を確認し、Amazon S3
バケットに保存されているアーティファクトを参照できます。ユーザーがオブジェクトをダウンロードしようとすると、アプリケーションはオブジェクトへのアクセス許可を確認し、ユーザーが example com などのカスタム
ドメイン名からオブジェクトをダウンロードできるようにする必要があります。
セキュリティ エンジニアがこの機能を実装する最も安全な方法は何ですか?
A. バケット ACL
を使用して、オブジェクトへの読み取り専用アクセスを構成します。一定時間が経過したらアクセスを解除してください。
B. IAM ポリシーを実装して、ユーザーに S3 バケットへの読み取りアクセスを付与します。

C. S3 署名付き URL の作成 アプリケーションを通じてユーザーに S3 署名付き URL を提供します。

D. Amazon CloudFront 署名付き URL を作成します。アプリケーションを通じて CloudFront 署名付き URL をユーザーに提供します。

Answer: D

Explanation:

For this scenario you would need to set up static website hosting because a custom domain name is listed as a requirement. "Amazon S3 website endpoints do not support HTTPS or access points. If you want to use HTTPS, you can use Amazon CloudFront to serve a static website hosted on Amazon S3." This is not secure.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/website-hosting-custom-domain-walkthrough.html CloudFront signed URLs allow much more fine-grained control as well as HTTPS access with custom domain names:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

QUESTION NO: 7

ある企業は、Amazon API Gateway を使用して REST API をユーザーに提供しています。API 開発者は、ログ ファイルを解析せずに API アクセス パターンを分析したいと考えています。

最小限の労力でこれらの要件を満たすことができる手順の組み合わせはどれですか? (2 つ選択してください。)

A. 必要な API ステージのアクセス ロギングを構成します。

B. API Gateway イベントの AWS CloudTrail 証跡送信先を設定します。userIdentity、userAgent、および sourceIPAddress フィールドでフィルターを構成します。

C. API Gateway ログの Amazon S3 送信先を設定します。Amazon Athena クエリを実行して、API アクセス情報を分析します。

D. Amazon CloudWatch Logs Insights を使用して、API アクセス情報を分析します。

E. 必要な API ステージで [詳細な CloudWatch メトリクスを有効にする] オプションを選択します。

Answer: C,D

QUESTION NO: 8

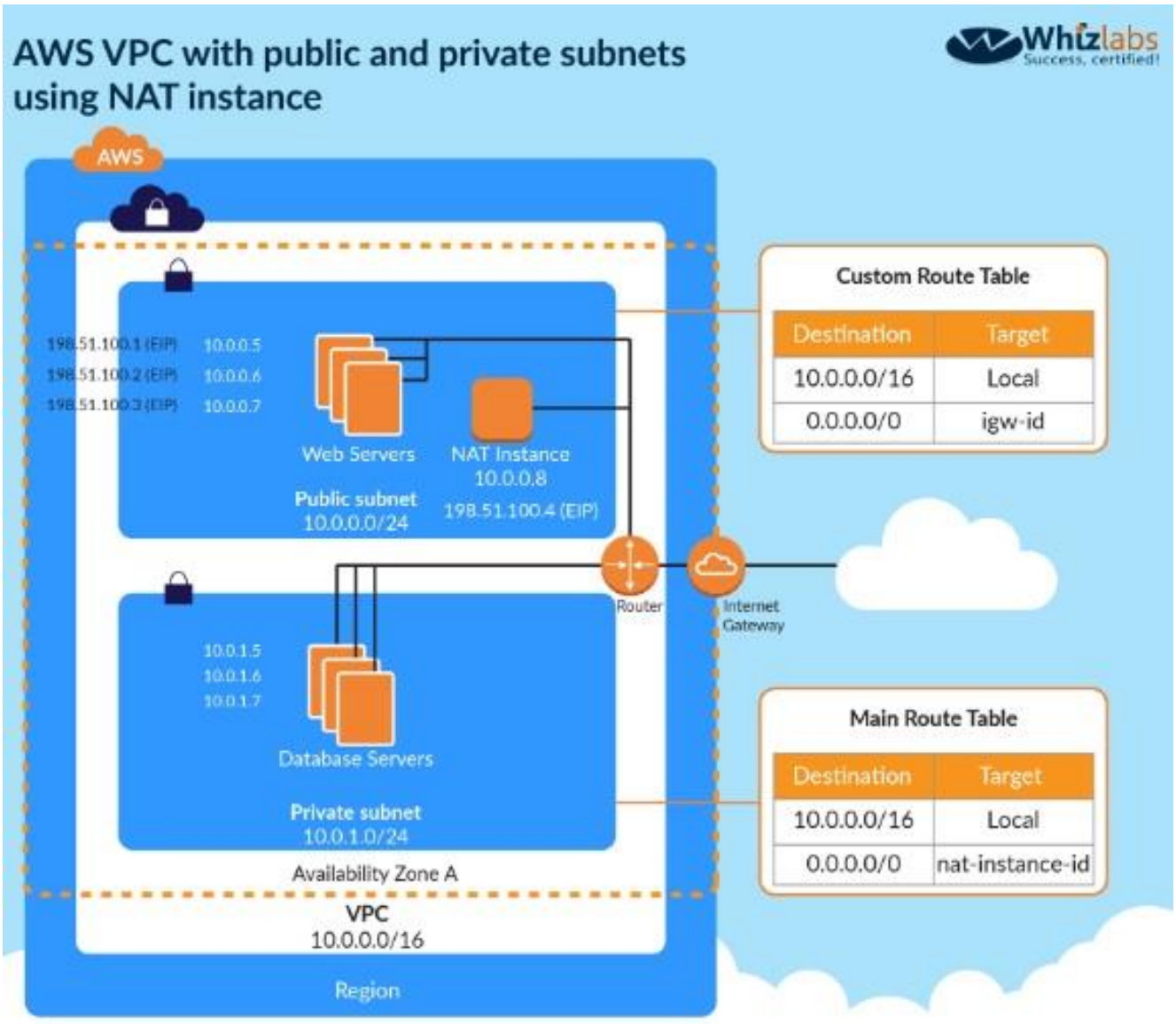
コンプライアンス上の理由から、セキュリティ エンジニアは、承認された最新のパッチが適用されていないインスタンスを一覧表示する週次レポートを作成する必要があります。また、エンジニアは、承認された最新の更新プログラムが適用されないままシステムが 30 日以上経過しないようにする必要があります。これらの目標を達成するための最も効率的な方法は何ですか?

A. Amazon inspector を使用して、最新のパッチが適用されていないシステムを特定し、30 日後にそれらのインスタンスを最新の AMI バージョンで再デプロイします。

B. Amazon EC2 Systems Manager を構成して、インスタンス パッチのコンプライアンスについて報告し、定義されたメンテナンス

ウィンドウ中に更新を適用します。
C. IAM CloudTrail togs を調べて、過去 30
日間に再起動されていないインスタンスがあるかどうかを判断し、それらのインスタンスを再デプロイします。
D. 最新の承認済みパッチで AMIs
を更新し、定義されたメンテナンス期間中に各インスタンスを再展開します。
Answer: B

QUESTION NO: 9
プライベートサブネットとパブリックサブネットを持つAmazonVPCがあり、その中にNATインスタンスサーバーがあります。
GITを介してアプリケーションをデプロイするS3からブートストラップスクリプトをダウンロードすることにより、起動時に自身を設定するEC2インスタンスのグループを作成しました。
次の設定のどれが私たちに最高レベルのセキュリティを与えるでしょうか？
以下のオプションから正しい答えを選択してください。
選んでください：
A.
パブリックサブネット内のEC2インスタンス、EIPなし、IGW経由で発信トラフィックをルーティング
B.
パブリックサブネット内のEC2インスタンス、割り当てられたEIP、NAT経由の発信トラフィックのルーティング
C.
プライベートサブネット内のEC2インスタンス、割り当てられたEIP、およびIGWを介した発信トラフィックのルーティング
D.
プライベートサブネット内のEC2インスタンス、EIPなし、NAT経由で発信トラフィックをルーティング
Answer: D
Explanation:
The below diagram shows how the NAT instance works. To make EC2 instances very secure, they need to be in a private sub such as the database server shown below with no EIP and all traffic routed via the NAT.



Options A and B are invalid because the instances need to be in the private subnet Option C is invalid because since the instance needs to be in the private subnet, you should not attach an EIP to the instance For more information on NAT instance, please refer to the below Link: http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuideA/PC Instance.html!
The correct answer is: EC2 instances in our private subnet no EIPs, route outgoing traffic via the NAT Submit your Feedback/Queries to our Experts

QUESTION NO: 10
IAM KMS
サービスを使用して定義された一連のキーがあります。いくつかのキーの使用を停止したいと考えていますが、現在どのサービスがキーを使用しているかわかりません。キーを今後使用しないようにするための安全なオプションは、次のうちどれですか。
選んでください：
A. いずれにせよ、削除までに 7 日間の待機期間があるため、キーを削除します。
B. キーを無効にします
C. キーのエイリアスを設定します

D. キーのキー マテリアルを変更します。

Answer: B

Explanation:

Option A is invalid because once you schedule the deletion and waiting period ends, you cannot come back from the deletion process.

Option C and D are invalid because these will not check to see if the keys are being used or not The IAM Documentation mentions the following Deleting a customer master key (CMK) in IAM Key Management Service (IAM KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.

For more information on deleting keys from KMS, please visit the below URL: https://docs.IAM.amazon.com/kms/latest/developereuide/deleting-keys.html The correct answer is: Disable the keys Submit your Feedback/Queries to our Experts

QUESTION NO: 11

ある企業は単一の AWS リージョンでワークロードを実行し、AWS Organizations を使用しています。セキュリティ

エンジニアは、ユーザーが他のリージョンでリソースを起動できないようにするソリューションを実装する必要があります。

運用オーバーヘッドを最小限に抑えながらこれらの要件を満たすソリューションはどれですか?

A. 指定されたリージョン内でのみアクションを許可する aws RequestedRegion 条件を持つ IAM ポリシーを作成します。ポリシーをすべてのユーザーにアタッチします。

B. 指定されたリージョンにないアクションを拒否する aws RequestedRegion 条件を持つ IAM ポリシーを作成します。このポリシーを AWS Organizations の AWS アカウントにアタッチします。

C. 必要なアクションを許可する aws RequestedRegion 条件を持つ IAM ポリシーを作成します。指定されたリージョン内のユーザーにのみポリシーをアタッチします。

D. 指定されたリージョンにないアクションを拒否する aws RequestedRegion 条件を持つ SCP を作成します。SCP を AWS Organizations の AWS アカウントにアタッチします。

Answer: D

Explanation:

Although you can use a IAM policy to prevent users launching resources in other regions. The best practice is to use SCP when using AWS organizations.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html#example-scp-deny-region

QUESTION NO: 12

開発者は、自分のアカウントで IAM CloudTrail が無効になっていると報告しました。セキュリティ

エンジニアがアカウントを調査したところ、現在のセキュリティ
ソリューションではイベントが検出されないことがわかりました。セキュリティ
エンジニアは、CloudTrail
構成に対する将来の変更を検出し、変更が発生したときにアラートを送信するソリューションを推奨する必要があります。
これらの要件を満たすために、セキュリティ エンジニアは何をする必要がありますか?

A. IAM Resource Access Manager (IAM RAM) を使用して、IAM CloudTrail
構成を監視します。Amazon SNS を使用して通知を送信します。

B. Amazon CloudWatch Events ルールを作成して、Amazon GuardDuty
の結果をモニタリングします。Amazon SNS を使用して E メール通知を送信します。

C. IAM サポートの IAM
アカウント設定でセキュリティ連絡先の詳細を更新し、疑わしいアクティビティが検出されたときにアラートを送信します。

D. Amazon Inspector を使用して、セキュリティの問題を自動的に検出します。Amazon SNS を使用してアラートを送信します。

Answer: B

QUESTION NO: 13
水道事業会社は、多数の Amazon EC2 インスタンスを使用して、水質を監視する 2,000
台のモノのインターネット (IoT) フィールド
デバイスの更新を管理しています。これらのデバイスには、それぞれ固有のアクセス資格情報があります。
運用上の安全性ポリシーでは、特定の資格情報へのアクセスが独立して監査可能である必要があります。
クレデンシャルのストレージを管理する最も費用対効果の高い方法は何ですか?

A. IAM Systems Manager を使用して、認証情報を Secure Strings
パラメータとして保存します。IAM KMS キーを使用して保護します。

B. IAM キー管理システムを使用して、資格情報の暗号化に使用されるマスター
キーを保存します。暗号化された認証情報は、Amazon RDS
インスタンスに保存されます。

C. IAM Secrets Manager を使用して認証情報を保存します。

D. サーバー側の暗号化を使用して、資格情報を Amazon S3 の JSON
ファイルに保存します。

Answer: A
Explanation:
https://docs.IAM.amazon.com/systems-manager/latest/userguide/parameter-store-advanced-parameters.html

QUESTION NO: 14
あなたの会社は、IAM で EC2 インスタンスの大部分をホストしています。EC2
インスタンスを管理する厳格なセキュリティ
ルールがあります。セキュリティ違反の可能性がある場合、基盤となる EC2
インスタンスを迅速に調査する必要があります。次のサービスのうち、侵害されたインスタンスを調査するためのテスト環境を迅速にプロビジョニングするのに役立つものはどれですか。

選んでください：
A. IAM クラウドウォッチ
B. IAM クラウドフォーメーション
C. IAM Cloudtrail
D. IAM 構成
Answer: B
Explanation:
The IAM Security best practises mentions the following
Unique to IAM, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can pre-configure instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean room.
Option A is incorrect since this is a logging service and cannot be used to provision a test environment Option C is incorrect since this is an API logging service and cannot be used to provision a test environment Option D is incorrect since this is a configuration service and cannot be used to provision a test environment For more information on IAM Security best practises, please refer to below URL:
https://d1.IAMstatic.com/whitepapers/architecture/IAM-Security-Pillar.pd1 The correct answer is: IAM Cloudformation Submit your Feedback/Queries to our Experts

QUESTION NO: 15
あなたのチームは、アプリケーションのAPIゲートウェイサービスを実験しています。
APIゲートウェイに対して行われた呼び出しの認証/承認に使用できるカスタムモジュールを実装する必要があります。どうすればこれを達成できますか？
選んでください：
A. 認証にリクエストパラメータを使用します
B. Lambdaオーソライザーを使用する
C. ゲートウェイ認証を使用します
D. APIゲートウェイでCORSを使用します
Answer: B
Explanation:
The IAM Documentation mentions the following
An Amazon API Gateway Lambda authorizer (formerly known as a custom authorize?) is a Lambda function that you provide to control access to your API methods. A Lambda authorizer uses bearer token authentication strategies, such as OAuth or SAML. It can also use information described by headers, paths, query strings, stage variables, or context variables request parameters.
Options A,C and D are invalid because these cannot be used if you need a custom authentication/authorization for calls made to the API gateway For more information on using the API gateway Lambda authorizer please visit the URL:
https://docs.IAM.amazon.com/apisateway/latest/developerguide/apieateway-use-lambda-authorizer.htmll The correct answer is: Use a Lambda authorizer Submit your

Feedback/Queries to our Experts

QUESTION NO: 16
ある企業が、新しい Amazon RDS データベース
アプリケーションを開発しました。会社は、転送中の暗号化と保存中の暗号化のために、R
OS
データベース資格情報を保護する必要があります。また、会社は資格情報を定期的に自動的
にローテーションする必要があります。
これらの要件を満たすソリューションはどれですか?
A. IAM Systems Manager Parameter Store
を使用して、データベース認証情報を保存します。資格情報の自動ローテーションを構成し
ます。
B. IAM Secrets Manager を使用して、データベース認証情報を保存します。資格情報の
automat* ローテーションを構成する
C. S3 管理の暗号化キー (SSE-S3) を使用したサーバー側の暗号化で構成された Amazon S3
バケットにデータベース認証情報を保存します。 IAM
データベース認証で認証情報をローテーションします。
D. データベース認証情報を Amazon S3 Glacier に保存し、S3 Glacier Vault Lock
を使用します IAM Lambda
関数を設定して、スケジュールされたバストで認証情報をローテーションします
Answer: A

QUESTION NO: 17
アプリケーションは、Amazon SQSからメッセージを取得するAmazon
EC2インスタンスで構築されています。
最近、IAMの変更が行われ、インスタンスはメッセージを取得できなくなりました。
最小限の特権を維持しながら、問題をトラブルシューティングするために実行するアクショ
ン。（2つ選択してください。）
A. MFAデバイスを設定し、インスタンスで使用されるロールに割り当てます。
B.
SQSリソースポリシーが、インスタンスで使用されるロールへのアクセスを明示的に拒否し
ていないことを確認します。
C.
インスタンスで使用されるロールにアタッチされたアクセスキーがアクティブであることを
確認します。
D. AmazonSQSFullAccess管理ポリシーをインスタンスで使用されるロールに添付します。
E.
インスタンスにアタッチされたロールに、キューへのアクセスを許可するポリシーが含まれ
ていることを確認します。
Answer: B,E

QUESTION NO: 18
企業のアプリケーションは Amazon EC2 で実行され、データは Amazon S3
バケットに保存されます。企業は、データが外部関係者に偶発的に公開される可能性を制限
するために、追加のセキュリティ制御を導入したいと考えています。この要件を満たすアク

ションの組み合わせはどれですか? (3 つ選択してください。)
A. Amazon S3 で管理された暗号化キー (SSE-S3)
を使用してサーバー側の暗号化を使用して、Amazon S3 のデータを暗号化します。
B. IAM KMS 管理の暗号化キー (SSE-KMS)
を使用したサーバー側の暗号化を使用して、Amazon S3 のデータを暗号化します。
C. 新しい Amazon S3 VPC エンドポイントを作成し、VPC のルーティング
テーブルを変更して新しいエンドポイントを使用する
D. Amazon S3 のブロック パブリック アクセス機能を使用します。
E. アプリケーション インスタンスからのアクセスのみを許可するようにバケット
ポリシーを構成します。
F. NACL を使用して、Amazon S3 へのトラフィックをフィルタリングします
Answer: B,C,E

QUESTION NO: 19
セキュリティ エンジニアは、Amazon S3 バケットのサンプル
バケットで暗号化が有効になっているにもかかわらず、バケットにアクセスできる人なら誰でもファイルを取得できることを発見しました。エンジニアは、割り当てられたフォルダーのみにアクセスできる各 IAM ユーザーにアクセスを制限したいと考えています。
これを達成するために、セキュリティ エンジニアは何をすべきですか?
A. IAM 管理の CMK IAM/s3 でエンベロープ暗号化を使用します。
B. に基づいて「kms:Decrypt」を付与するキー ポリシーを使用して、顧客管理の CMK
を作成します。
「${IAM:username}」変数。
C. ユーザーごとに顧客管理の CMK を作成します。各ユーザーを、対応するキー
ポリシーにキー ユーザーとして追加します。
D. 該当する IAM ポリシーを変更して、「リソース」への S3 アクセスを許可します。
"arn:IAM:s3:::examplebucket/${IAM:ユーザー名}/*"
Answer: B

QUESTION NO: 20
情報技術部門は、クラシックロードバランサーの使用を停止し、コストを節約するためにApplication Load
Balancerに切り替えました。切り替え後、古いデバイスの一部のユーザーはWebサイトに接続できなくなります。
この状況の原因は何ですか？
A. Application Load Balancerは古いWebブラウザーをサポートしていません。
B. Perfect Forward Secrecy設定が正しく構成されていません。
C. 中間証明書はApplication Load Balancer内にインストールされます。
D. Application Load Balancerの暗号スイートが接続をブロックしています。
Answer: D
Explanation:
https://docs.IAM.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

QUESTION NO: 21
アプリケーションは、IAM SDK を使用して IAM
サービスを呼び出します。アプリケーションは、関連付けられた IAM ロールを持つ Amazon EC2 インスタンスで実行されます。アプリケーションが Amazon S3
バケット内のオブジェクトにアクセスしようとしたとき。管理者は次のエラー
メッセージを受け取ります。 HTTP 403: アクセスが拒否されました。
この問題をトラブルシューティングするために、管理者はどの手順を組み合わせて実行する必要がありますか? (3 つ選択してください。)
A. EC2 インスタンスのセキュリティ グループが S3
アクセスを承認していることを確認します。
B. KMS キー ポリシーで、この IAM 原則の KMS
キーの復号化アクセスが許可されていることを確認します。
C. オブジェクトへのアクセスを拒否するステートメントがないか、S3 バケット
ポリシーを確認します。
D. EC2 インスタンスが正しいキー ペアを使用していることを確認します。
E. EC2 インスタンスに関連付けられた IAM ロールに適切な権限があることを確認します。
F. インスタンスと S3 バケットが同じリージョンにあることを確認します。
Answer: B,C,E

QUESTION NO: 22
会社は IAM Secrets Manager を使用して、CMK を使用して暗号化され、セキュリティ
アカウント 111122223333
に保存されているシークレットを保存しています。会社の実稼働アカウントの 1
つ。444455556666、セキュリティ アカウント 111122223333
からシークレット値を取得する必要があります。セキュリティ エンジニアは、セキュリティ アカウントのシークレットに最小特権アクセスに基づいてポリシーを適用し、運用アカウントがシークレット値のみを取得できるようにする必要があります。
セキュリティ エンジニアはどのポリシーを適用する必要がありますか?

A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
}
```

B.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

C.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

D.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
```

A. オプション A

B. オプション B
C. オプション C
D. オプション D
Answer: A

QUESTION NO: 23
監査により、ある会社の Amazon EC2 インスタンス セキュリティ グループが無制限の受信 SSH
トラフィックを許可することで、会社のポリシーに違反していると判断されました。セキュリティ
エンジニアは、このような違反を管理者に通知するほぼリアルタイムの監視およびアラートソリューションを実装する必要があります。
最も運用効率が高く、これらの要件を満たすソリューションはどれですか?
A. 毎日実行され、Network Reachability パッケージを使用する定期的な Amazon Inspector 評価実行を作成します。評価の実行が開始されたときに IAM Lambda 関数を呼び出す Amazon CloudWatch
ルールを作成します。完了時に評価実行レポートを取得して評価するように Lambda 関数を設定します。無制限の着信 SSH トラフィックに違反がある場合に、Amazon Simple Notification Service (Amazon SNS) 通知を発行するように Lambda 関数も設定します。
B. 準拠していないセキュリティ グループの構成変更によって呼び出される、restricted-ssh IAM Config マネージド ルールを使用します。IAM Config
修復機能を使用して、メッセージを Amazon Simple Notification Service (Amazon SNS) トピックに発行します。
C. VPC の VPC フロー ログを構成します。Amazon CloudWatch Logs
グループを指定します。新しいログエントリを解析し、ポート 22
での接続の成功を検出し、Amazon Simple Notification Service (Amazon SNS)
を介して通知を発行する IAM Lambda 関数に CloudWatch Logs
グループをサブスクライブします。
D. 毎日実行され、Security Best Practices パッケージを使用する定期的な Amazon Inspector 評価実行を作成します。評価の実行が開始されたときに IAM Lambda 関数を呼び出す Amazon CloudWatch
ルールを作成します。完了時に評価実行レポートを取得して評価するように Lambda 関数を設定します。無制限の着信 SSH トラフィックに違反がある場合に、Amazon Simple Notification Service (Amazon SNS) 通知を発行するように Lambda 関数も設定します。
Answer: A

QUESTION NO: 24
ある会社が、AutoScalingグループのAmazonEC2インスタンスでアプリケーションを実行しています。
アプリケーションはログをローカルに保存しますセキュリティエンジニアは、スケールインイベント後にログが失われたことに気づきました。セキュリティエンジニアは、ログデータの耐久性と可用性を確保するためのソリューションを推奨する必要があります。監査の目的で、すべてのログを最低1年間保持する必要があります。セキュリティエンジニアは何を推奨する必要がありますか。

A. Auto Scalingライフサイクル内で、EC2インスタンスが作成されるたびに、Amazon Elastic Block Store（Amazon EBS）ログボリュームを作成してアタッチするフックを追加します。インスタンスが終了すると、ログレビューのためにEBSボリュームを別のインスタンスに再接続できます。

B. Amazon Elastic File System（Amazon EFS）ファイルシステムを作成し、Auto Scaling起動テンプレートのユーザーデータセクションにコマンドを追加して、EC2インスタンスの作成中にEFSファイルシステムをマウントします。インスタンスでプロセスを構成して、ログを1回コピーします。インスタンスのAmazonElastic Block Store（Amazon EBS）ボリュームからEFSファイルシステムのディレクトリまでの1日。

C. AutoScalingグループで使用されるAMIにAmazonCloudWatchエージェントをビルドします。レビューのためにログをAmazonCloudWatchLogsに送信するようにCloudWatchエージェントを設定します。

D. Auto Scalingライフサイクル内で、終了状態遷移にライフサイクルフックを追加し、Amazon Simple Notification Service（Amazon SNS）へのライフサイクル通知を使用してエンジニアリングチームに警告します。インスタンスが終了する前にセキュリティログを手動で確認できるように、フックを1時間Termination：Wait状態のままにするように構成します。

Answer: B

QUESTION NO: 25

企業の IAM アカウントは、約 300 人の IAM ユーザーで構成されています。現在、100 人の IAM ユーザーが S3 に対して無制限の権限を持つには、アクセスの変更が必要であるという義務があります。システム管理者として、個々のユーザーレベルでポリシーを適用する必要がないように、これを効果的に実装するにはどうすればよいでしょうか?

選んでください：

A. 新しいロールを作成し、各ユーザーを IAM ロールに追加します

B. IAM グループを使用し、ロールに基づいてユーザーを別のグループに追加し、ポリシーをグループに適用します。

C. ポリシーを作成し、JSON スクリプトを使用して複数のユーザーに適用します

D. 各ユーザーの IAM アカウント ID を含む無制限アクセスの S3 バケットポリシーを作成します。

Answer: B

Explanation:

Option A is incorrect since you don't add a user to the IAM Role

Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group For more information on IAM Groups, just browse to the below URL:

https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group Submit your Feedback/Queries to our Experts

QUESTION NO: 26
ある企業には、各ビジネスユニットの専用アカウントを含む AWS Organizations の組織があります。同社は、最上位アカウントの単一の Amazon S3 バケット内のアカウントからすべての AWS CloudTrail ログを収集しています。会社の IT ガバナンス チームは、トップレベルのアカウントにアクセスできます。セキュリティ エンジニアは、各ビジネス ユニットが独自の CloudTrail ログにアクセスできるようにする必要があります。
セキュリティ エンジニアは、他の各アカウントの最上位アカウントに IAM ロールを作成します。セキュリティ エンジニアはロールごとに IAM ポリシーを作成し、それぞれのログのプレフィックスを持つ S3 バケット内のオブジェクトへの読み取り専用アクセス許可を許可します。
そのアカウントの IAM ユーザーにログの読み取りを許可するには、各ビジネス ユニット アカウントでセキュリティ エンジニアが実行する必要があるアクションはどれですか?
A. IAM ユーザーにポリシーをアタッチして、ユーザーがトップレベルのアカウントで作成されたロールを引き受けることを許可します。ポリシーでロールの ARN を指定します。
B. 最上位アカウントに権限を付与する SCP を作成します。
C. ビジネス ユニット アカウントのルート アカウントを使用して、最上位アカウントで作成されたロールを引き受けます。ポリシーでロールの ARN を指定します。
D. 最上位アカウントの IAM ロールの認証情報をビジネス ユニット アカウントの IAM ユーザーに転送します。
Answer: A
Explanation:
To allow an IAM user in one AWS account to access resources in another AWS account using IAM roles, the following steps are required:
Create a role in the AWS account that contains the resources (the trusting account) and specify the AWS account that contains the IAM user (the trusted account) as a trusted entity in the role's trust policy. This allows users from the trusted account to assume the role and access resources in the trusting account.
Attach a policy to the IAM user in the trusted account that allows the user to assume the role in the trusting account. The policy must specify the ARN of the role that was created in the trusting account.
The IAM user can then switch roles or use temporary credentials to access the resources in the trusting account.
Verified Reference:
https://repost.aws/knowledge-center/cross-account-access-iam
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

QUESTION NO: 27
会社のセキュリティ ポリシーでは、すべての VPC で VPC フロー
ログを有効にする必要があります。セキュリティ エンジニアは、コンプライアンスのために
VPC リソースを監査するプロセスを自動化しようとしています。
エンジニアが取るべきアクションの組み合わせは？(2つ選んでください。)
A. 特定の VPC でフロー ログが有効になっているかどうかを判断する IAM Lambda
関数を作成します。
B. 会社の IAM アカウントの VPC ごとに IAM Config 構成アイテムを作成します。
C. IAM:: Lambda:: Function のリソース タイプで IAM Config マネージド
ルールを作成します。
D. IAM Config によって発行されたイベントでトリガーする Amazon CloudWatch イベント
ルールを作成します。
E. IAM Config カスタム ルールを作成し、評価ロジックを含む IAM Lambda
関数に関連付けます。
Answer: A,E
Explanation:
https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-IAM-config-rules-2e53b09006de

QUESTION NO: 28
企業は重要なデータをS3バケットでホストします。バケットに適切な権限が割り当てられていても、データの削除が心配されています。バケットのデータ削除のリスクを制限するためにどのような対策を講じることができますか。以下のオプションから2つの回答を選択してください。
A. S3バケットでバージョン管理を有効にします
B. バケット内のオブジェクトの保存データを有効にします
C. バケットポリシーでMFA削除を有効にする
D. バケット内のオブジェクトの転送中のデータを有効にします
Answer: A,C
Explanation:
One of the IAM Security blogs mentions the followinj
You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your IAM accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket.
Option B is invalid because enabling encryption does not guarantee risk of data deletion.
Option D is invalid because this option does not guarantee risk of data deletion.
For more information on IAM S3 versioning and MFA please refer to the below URL:
https://IAM.amazon.com/blogs/security/securing-access-to-IAM-using-mfa-part-3/ The correct answers are: Enable versioning on the S3 bucket Enable MFA Delete in the bucket policy
Submit your Feedback/Queries to our Experts

QUESTION NO: 29
企業には何百もの IAM アカウントがあり、これらすべてのアカウントの IAM CloudTrail

を収集するために使用される一元化された Amazon S3 バケットがあります。セキュリティエンジニアは、企業の IAM アカウントで証跡が最初に有効化されたときから 3 年前にさかのぼる CloudTrail ログに対してアドホックキューを実行できるようにするソリューションを作成したいと考えています。
会社は、管理オーバーヘッドを最小限に抑えてこれをどのように達成する必要がありますか?

A. MapReduce ジョブを使用する Amazon EMP クラスターを実行して、CloudTrail 証跡を調べます。

B. CloudTrail コンソールのイベント履歴/機能を使用して、CloudTrail 証跡を照会します。

C. CloudTrail 証跡を照会する IAM Lambda 関数を作成する CloudTrail S3 バケットで新しいファイルが作成されるたびに実行されるように Lambda 関数を設定します。

D. CloudTrail 証跡が書き込まれている S3 バケットでツールを使用する Amazon Athena テーブルを作成し、Athena を使用して証跡に対してクエリを実行します。

Answer: D

QUESTION NO: 30
あなたの会社では、データの保存に S3 バケットを利用しています。すべてのサービスでログを有効にする必要があるという会社のポリシーがあります。IAM アカウントで作成された S3 バケットに対してログが常に有効になっていることを確認するにはどうすればよいですか? 選んでください：

A. IAM Inspector を使用してすべての S3 バケットを検査し、有効になっていない場合はログを有効にします

B. IAM Config Rules を使用して、バケットのロギングが有効になっているかどうかを確認します

C. IAM Cloudwatch メトリクスを使用して、バケットのロギングが有効になっているかどうかを確認します

D. IAM Cloudwatch ログを使用して、バケットのロギングが有効になっているかどうかを確認します

Answer: B
Explanation:
This is given in the IAM Documentation as an example rule in IAM Config Example rules with triggers Example rule with configuration change trigger
1. You add the IAM Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. IAM Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and IAM Config evaluates whether the bucket is compliant against the rule.
Option A is invalid because IAM Inspector cannot be used to scan all buckets Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.
For more information on Config Rules please see the below Link:
https://docs.IAM.amazon.com/config/latest/developerguide/evaluate-config-rules.html The

correct answer is: Use IAM Config Rules to check whether logging is enabled for buckets
Submit your Feedback/Queries to our Experts